TECHNICAL WHITE PAPER

Avaya G700 Media Gateway Security Features Overview

Version: **1.1**

Date: **February 3, 2004**

CID: **102412**

Author: **Avaya Technology and Consulting**
Corporate Systems Engineering

Abstract:

The Avaya G700 Media Gateway Security Features Overview is a sister document to the Avaya G350 Media Gateway Security Features Overview (CID: 102411). As such, they both follow the same template of questions.

One distinguishing factor of the G700 from the standalone G350 architecture is that it has a modular expansion bay and is stackable with other Avaya infrastructure components. This enables additional features and functionality. This security features overview assumes the G700 is configured as a standalone unit without an X330WAN module in the expansion bay.

The Avaya G700 Media Gateway provides a variety of features which can be used to enhance security. The goal of this white paper is to summarize the general product documentation and focus on those features.

P330 SW Version 4.0.17, FW version 21.20.1

©2004 Avaya Inc. All Rights Reserved. Avaya and the Avaya logo are trademarks of Avaya Inc. and may be registered in certain jurisdictions. All trademarks identified by ® and ™ are registered trademarks or trademarks respectively, of Avaya Inc. All other registered trademarks or trademarks are property of their respective owners.

Table of Contents
(click on link to view more detailed information)

Access Control Lists / Denial of Service (DOS) Protection

1. Access Control List's
2. Denial of Service Protection

Auditing Transactions / Administration

3. CLI Command Auditing (via Syslog)
4. Show Currently Logged on Administrators

Authentication Credentials / RADIUS

5. Default User Accounts
6. Username/Password Characteristics
7. RADIUS Switch Administrator Authentication

CLI Inactivity Timeout and Pre/Post Login Banners

8. Idle Timeout
9. Banners

Network Client/Server applications

10. Show Protocol
11. Enable/Disable Network Services
12. Client / Server Network Tools
13. Default Listening Ports (UDP/TCP)
14. SSH/SCP/HTTPS/SNMPv3 Support

SNMP / Syslog Configuration

15. SNMP Defaults
16. Syslog / SNMP Output
17. Allowed Managers

©2004 Avaya Inc. All Rights Reserved. Avaya and the Avaya logo are trademarks of Avaya Inc. and may be registered in certain jurisdictions. All trademarks identified by ® and ™ are registered trademarks or trademarks respectively, of Avaya Inc. All other registered trademarks or trademarks are property of their respective owners.

Access Control Lists / Denial of Service (DOS) Protection

1. Access Control Lists

Unlike the G350 Media Gateway, Access Control Lists are not native to the G700 (a layer 2 device) and require a X330WAN expansion module in the expansion bay or other L3 switch in a stack.

Return to Table of Contents

2. DOS Protection

Unlike the G350 Media Gateway, this functionality is not available on the G700.

Return to Table of Contents

©2004 Avaya Inc. All Rights Reserved. Avaya and the Avaya logo are trademarks of Avaya Inc. and may be registered in certain jurisdictions. All trademarks identified by ® and ™ are registered trademarks or trademarks respectively, of Avaya Inc. All other registered trademarks or trademarks are property of their respective owners.

3. CLI Command Auditing (via Syslog)

Unlike the G350, the G700 does not support Syslog.

Return to Table of Contents

4. Show Currently Logged on Administrators

```
G700Parkland-1(super)# show secure current

   IP Address                Time Since Last Request(In Sec)
  -------------             ------------------------------------

    192.168.1.100               5

G700Parkland-1(super)#
```

Return to Table of Contents

©2004 Avaya Inc. All Rights Reserved. Avaya and the Avaya logo are trademarks of Avaya Inc. and may be registered in certain jurisdictions. All trademarks identified by ® and ™ are registered trademarks or trademarks respectively, of Avaya Inc. All other registered trademarks or trademarks are property of their respective owners.

Authentication Credentials / RADIUS

5. Usernames

By default there is only a single user account, named root, with password root, which accesses the administrator level. You cannot delete this basic user account, nor modify its access level. But you can modify its basic password.

```
G700-002(super)# show username

         User account                      password                access-type
------------------------------  --------------------------------  ---------
root                            *****                               admin
```

Return to Table of Contents

6. Username/Password Characteristics

- **Username: minimum 4 characters, maximum 31 characters**
- **Password: minimum 4 characters, maximum 31 characters (all keyboard characters are valid)**
- **There can be up to 3 password entry attempts at login before the session is terminated**
- **Up to 10 unique "local" usernames can be configured on the G700**

When you start to use Avaya G700 Manager or the CLI, you must enter a username. The username that you enter sets your privilege level. The commands that are available to you during the session depend on your privilege level. If you use RADIUS authentication, the RADIUS server sets your privilege level.

Privilege level	Purpose
Read-only	View configuration parameters
Read-write	View and change configuration parameters
Admin	View and change configuration parameters and security parameters

- You can use Read-only privilege level to view configuration parameters.
- You can use Read-write privilege level to view and change all configuration parameters except those related to security. For example, you cannot change a password with Read-write privilege level.
- You can use Admin privilege level to view and change all configuration parameters, including parameters related to security. Use Admin privilege level only when you need to change configuration that is related to security, such as adding a new user accounts and setting the device policy manager source.

©2004 Avaya Inc. All Rights Reserved. Avaya and the Avaya logo are trademarks of Avaya Inc. and may be registered in certain jurisdictions. All trademarks identified by ® and ™ are registered trademarks or trademarks respectively, of Avaya Inc. All other registered trademarks or trademarks are property of their respective owners.

```
Username commands:
-----------------------------------------------------------------------------
Usage: username <name> password <passwd> access-type {read-only|read-
write|admin}
```

- Does the ability exist to force a minimum length username and/or password (other than default minimum of 4 characters)? No. However, this can be accomplished by using an external authentication database such as RADIUS.
- Does the configuration file include user account passwords or SNMP Community Strings? The configuration file does not include SNMP community strings and user/password data.
- Are there any “undocumented” usernames or SNMP community strings? No. All "diag" accounts are in-accessible without first logging into the G700 via a super-user account first. Backdoor password recovery exists but can only be used via a direct connection to the console port. It can also be disabled.
- Is there any way to enforce password aging on “local” accounts used to administer the G700? No. However, this can be accomplished by using an external authentication database such as RADIUS.
- Is there any way to enforce account "lock-out" after user inactivity of that account – i.e. user has not logged in for 60 days? No. However, this can be accomplished by using an external authentication database such as RADIUS.
- Any way to enforce "lock-out" of accounts after excessive retries? Using RADIUS only. No. However, this can be accomplished by using an external authentication database such as RADIUS.
- Any way for the G700 to prevent simple/dictionary words from being chosen as passwords? No. However, this can be accomplished by using an external authentication database such as RADIUS.
- Any way to age passwords? And if so, any way for the G700 to prevent password reuse, and if so how many past passwords are stored? No. However, this can be accomplished by using an external authentication database such as RADIUS.

Return to Table of Contents

7. RADIUS Switch Administrator Authentication

If your network has a RADIUS server, you can configure the Avaya G700 Media Gateway to use RADIUS authentication. A RADIUS server provides centralized authentication service for many devices on a network. When you use RADIUS authentication, you do not need to configure usernames and passwords on the G700. When you try to access the G700, the G700 searches for your username and password in its own database first. If it does not find them, it activates RADIUS authentication.

©2004 Avaya Inc. All Rights Reserved. Avaya and the Avaya logo are trademarks of Avaya Inc. and may be registered in certain jurisdictions. All trademarks identified by ® and ™ are registered trademarks or trademarks respectively, of Avaya Inc. All other registered trademarks or trademarks are property of their respective owners.

```
G700Parkland-1(super)# show radius authentication

Mode:                   Enable
Primary-server:         192.168.1.205
Secondary-server:       172.16.1.205
Retry-number:           4
Retry-time:             5
UDP-port:               1812
shared-secret:          secret

G700Parkland-1(super)#
```

Return to Table of Contents

©2004 Avaya Inc. All Rights Reserved. Avaya and the Avaya logo are trademarks of Avaya Inc. and may be registered in certain jurisdictions. All trademarks identified by ® and ™ are registered trademarks or trademarks respectively, of Avaya Inc. All other registered trademarks or trademarks are property of their respective owners.

CLI Inactivity Timeout and Pre/Post Login Banners

8. Idle Timeout

```
G700Parkland-1(super)# show timeout

CLI timeout is 15 minutes

G700Parkland-1(super)#

G700Parkland-1(super)# set logout

Session will be automatically logged out after 15 minutes of idle time.

G700Parkland-1(super)#
```

Return to Table of Contents

9. Banners

```
G700Parkland-1(super)# set welcome message ?

Set welcome message commands:
------------------------------------------------------------------------------
Usage: set welcome message [string]
      [string] : string to be used as the welcome message
                 blank - restore default string

G700Parkland-1(super)#
```

Return to Table of Contents

©2004 Avaya Inc. All Rights Reserved. Avaya and the Avaya logo are trademarks of Avaya Inc. and may be registered in certain jurisdictions. All trademarks identified by ® and ™ are registered trademarks or trademarks respectively, of Avaya Inc. All other registered trademarks or trademarks are property of their respective owners.

Network Client/Server applications

10. Show Protocol

Command not available on G700

Return to Table of Contents

11. Enable/Disable Services

- You cannot perform ICMP redirect and ACL (since it's a L2 only device)
- You cannot shutdown the Telnet server
- You cannot disable the Telnet client, SNMP Agent, or HTTP Server
- An FTP client does not exist on the G700
- You cannot toggle recovery password (but you can only do the recovery if you are directly connected to the G700 serial console)

Return to Table of Contents

12. Client / Server Network Tools

Telnet Client in "session mgc" always enabled (cannot be disabled)
Telnet Server – always enabled (cannot be disabled)
HTTP Server – always enabled (cannot be disabled)
SNMP Agent – always enabled (Read, Read-Write, Trap) (cannot be disabled)

Return to Table of Contents

13. Default Listen Ports

```
[root@babybeluga2 root]# nmap -sU 192.168.1.30

Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at 2004-01-06 20:43 EST
Interesting ports on 192.168.1.30:
(The 1474 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE
69/udp   open  tftp
161/udp  open  snmp
1030/udp open  iad1
1812/udp open Untitled 1 radius

Nmap run completed -- 1 IP address (1 host up) scanned in 10.902 seconds
[root@babybeluga2 root]#



[root@babybeluga2 root]# nmap -sT 192.168.1.30
```


©2004 Avaya Inc. All Rights Reserved. Avaya and the Avaya logo are trademarks of Avaya Inc. and may be registered in certain jurisdictions. All trademarks identified by ® and ™ are registered trademarks or trademarks respectively, of Avaya Inc. All other registered trademarks or trademarks are property of their respective owners.

```
Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at 2004-01-06 20:43 EST
Interesting ports on 192.168.1.30:
(The 1654 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE
23/tcp   open  telnet
80/tcp   open  http
4000/tcp open  remoteanything

Nmap run completed -- 1 IP address (1 host up) scanned in 3.108 seconds
```

TCP/4000 appears open (if you do port scan) but this port is blocked by the switches Operating System.

Return to Table of Contents

14. SSH/SCP/HTTPS/SNMPv3 Support?

There are no plans to support SSH/SCP, HTTPS or SNMPv3.

Return to Table of Contents

©2004 Avaya Inc. All Rights Reserved. Avaya and the Avaya logo are trademarks of Avaya Inc. and may be registered in certain jurisdictions. All trademarks identified by ® and ™ are registered trademarks or trademarks respectively, of Avaya Inc. All other registered trademarks or trademarks are property of their respective owners.

SNMP / Syslog Configuration

15. SNMP Defaults

```
G700Parkland-1(super)# show snmp

Authentication trap disabled

Community-Access     Community-String
----------------     ----------------
read-only            public
read-write           public
trap                 public

Trap-Rec-Address     Status       Traps Configured
----------------     --------     ----------------
G700Parkland-1(super)#

G700Parkland-1(super)# set snmp ?
Set snmp commands:
--------------------------------------------------------------------------------
set snmp community                 Set SNMP community string
set snmp trap                      Set snmp trap on the system or add an
entry into the SNMP trap receiver
set snmp retries                   Set The SNMP Retries Number
set snmp timeout                   Set The SNMP Timeout

G700Parkland-1(super)#
```

Return to Table of Contents

16. Syslog /SNMP Output

```
Syslog not available on G700

G700Parkland-1(super)# set snmp trap enable ?
Set snmp trap enable commands:
--------------------------------------------------------------------------------
set snmp trap enable auth                      Enable snmp authentication
trap

* The auth trap is global and applies to all the trap receivers, while other
traps can be set on or off per trap receiver.

G700Parkland-1(super)#

G700Parkland-1(super)# set snmp trap enable ?
Set snmp trap enable commands:
--------------------------------------------------------------------------------
set snmp trap enable auth                      Enable snmp authentication
trap
```


©2004 Avaya Inc. All Rights Reserved. Avaya and the Avaya logo are trademarks of Avaya Inc. and may be registered in certain jurisdictions. All trademarks identified by ® and ™ are registered trademarks or trademarks respectively, of Avaya Inc. All other registered trademarks or trademarks are property of their respective owners.

```
G700Parkland-1(super)# show snmp

Authentication trap enabled

Community-Access     Community-String
----------------     ----------------
read-only            public
read-write           public
trap                 public

Trap-Rec-Address     Status       Traps Configured
----------------     --------     ----------------
192.168.1.100        Enabled      config
                                  fault
                                  trafic_threshold
                                  module_De-Enrollment
                                  module_Enrollment
                                  delete_SW_redundancy_entry
                                  create_SW_redundancy_entry
                                  temperature_warning
                                  general_threshold
                                  cam_change
                                  duplicate_ip
                                  ip_vlan_violation
                                  link_aggregation_connection_fault
                                  link_aggregation_connection_return
                                  link_aggregation_partial_fault
                                  link_aggregation_partial_return
                                  delete_lag
                                  create_new_lag
                                  active_policy_list_change
                                  policy_access_control_violation
                                  BUPS_module_fault
                                  BUPS_module_fault_return
                                  BUPS_fans_module_fault
                                  BUPS_fans_module_fault_return
                                  fans_module_fault
                                  fans_module_fault_return
                                  cascade_up_connection_fault
                                  Cascade_up_connection_fault_return
                                  Cascade_down_connection_fault_return
                                  Cascade_down_connection_fault

G700Parkland-1(super)#

Authentication Failure Traps:

Wrong SNMP Community String:

0000  30 2B 02 01 00 04 06 70 75 62 6C 69 63 A4 1E 06  0+.....public...
0010  09 2B 06 01 04 01 51 11 01 11 40 04 C0 A8 01 1E  .+....Q...@.....
0020  02 01 04 02 01 00 43 03 1B 77 4D 30 00           ......C..wM0.

Frame Length: 45 bytes
```


©2004 Avaya Inc. All Rights Reserved. Avaya and the Avaya logo are trademarks of Avaya Inc. and may be registered in certain jurisdictions. All trademarks identified by ® and ™ are registered trademarks or trademarks respectively, of Avaya Inc. All other registered trademarks or trademarks are property of their respective owners.

```
Community: public
OID: .1.3.6.1.4.1.81.17.1.17
Address: 192.168.1.30
sysUpTime: 0 days, 05:00:00
Generic: 4 - Authentication Failure
Specific: 0

Wrong Telnet Password:

No Event (*)
(*) Note: this is a bug in the current G700 version (based on P330 V4.0)
there is no set date for resolution.

Wrong HTTP Password:

No Event (*)
(*) Note: This is a bug in the current G700 version (based on P330 V4.0)
there is no set date for resolution.
```

Return to Table of Contents

17. Allowed Managers

```
G700Parkland-1(super)# set allowed ?
Set allowed commands:
------------------------------------------------------------------------------
set allowed managers                  When set to enabled - only managers
with ip address specified in the allowed table will be able to access the
device

G700Parkland-1(super)#
```

This command will restrict SNMP, HTTP and Telnet access to the G700 for the defined allowed managers IP addresses. The identification of an “Allowed Manager” is done by checking the Source IP address of the packets.

You can configure up to 20 Allowed Mangers by adding or removing their IP address from the Allowed Managers List.

Return to Table of Contents

*****END*****

©2004 Avaya Inc. All Rights Reserved. Avaya and the Avaya logo are trademarks of Avaya Inc. and may be registered in certain jurisdictions. All trademarks identified by ® and ™ are registered trademarks or trademarks respectively, of Avaya Inc. All other registered trademarks or trademarks are property of their respective owners.